IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

UNITED STATES OF AMERICA,

Plaintiff,

v. // CRIMINAL ACTION NO. 1:16CR18
(Judge Keeley)

MICHAEL P. LOUGH,

Defendant.

MEMORANDUM OPINION AND ORDER DENYING
DEFENDANT'S MOTION TO SUPPRESS EVIDENCE [DKT. NO. 43]

Pending before the Court is the motion to suppress filed by the defendant, Michael P. Lough ("Lough"), seeking to suppress evidence seized pursuant to a warrant issued by United States Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. For the reasons that follow, the Court **DENIES** the motion (dkt. no. 43).

I. BACKGROUND

In December of 2014, the Federal Bureau of Investigation ("FBI") became aware that a website operating on the "dark web" under the moniker "Playpen" was trafficking in child pornography. Playpen operated on the TOR network,[1] which enables online users to access websites, including Playpen and other child pornography

[1]"TOR" is an acronym for "the onion router." The TOR network provides online anonymity to users by "bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user." Dkt. No. 19-1 at 11-12.

sites, anonymously and beyond traditional law enforcement detection techniques by hiding their IP addresses and identities.

On February 20, 2015, the FBI seized the computer server that hosted the Playpen website from a web-hosting facility in Renoir, North Carolina. Dkt. No. 19 at 2. The FBI removed the server to a facility in the Eastern District of Virginia, at which point it obtained a search warrant from Magistrate Judge Buchanan, which authorized the use of a network investigation technique ("NIT"). Dkt. No. 19-1. Rather than simply disabling the server, however, the FBI continued to administer it for thirteen days in an effort to obtain information about individuals seeking and disseminating child pornography. Whenever a user logged into the Playpen website with their username and password, the NIT program initiated software triggering the user's computer to reveal its IP address and other identifying information.

Utilizing the NIT, the FBI determined that a user living in Fairmont, West Virginia, with the user name "2tots," had logged into the Playpen website and accessed child pornography. Dkt. No. 20-2 at 18-19. Records compiled by the Playpen server established that "2Tots" had been logged on for approximately seventeen hours between November 23, 2014 and March 1, 2015. Id. at 19. The NIT revealed the

IP address from which "2Tots" was logging into the Playpen site.[2] Id. An administrative subpoena served on Frontier Communications Corporation established that the IP address for "2tots" belonged to Lough's account, which was registered to a street address later determined to belong to him. Id. at 20. Based on this information, FBI Special Agent Ryan ("SA Ryan") sought a search warrant for Lough's home (the "Residential warrant"), which United States Magistrate Judge James E. Seibert of this district issued on July 14, 2015. Dkt. No. 19 at 3. SA Ryan and other agents then raided Lough's home, where they seized multiple pieces of evidence suspected of containing child pornography. Id.

The government filed a one-count Information against Lough on March 15, 2016, following which he appeared before United States Magistrate Judge Michael J. Aloi on March 23, 2016 for an initial appearance, arraignment, and plea hearing. At the hearing, Lough was placed under oath and waived his right of indictment. Id. Pursuant to Fed. R. Crim. P. 11(3), the government called SA Ryan, who recounted the factual basis for Lough's guilty plea. Lough then acknowledged the facts as stated by SA Ryan, admitted to the

[2]The NIT also revealed the "host and logon name" for Lough's computer, which was "mikeandjulie." Dkt. No. 20-2 at 20. The host and logon name was not necessary for securing the subpoena on Frontier Communications nor was it needed to secure the Residential warrant.

elements of the charge in the information, and entered his guilty plea.

Thereafter, on May 4, 2016, Lough moved to withdraw his guilty plea. Based on a recent opinion by another district court granting a defendant's motion to suppress evidence gathered through the same NIT warrant that is the subject of this case, Lough believed he too could move to suppress such evidence (dkt. no. 17). After due consideration of his motion, on August 25, 2016, the Court vacated his guilty plea and provided the parties with a briefing schedule on the anticipated motion to suppress (dkt. no. 35).

On September 12, 2016, Lough moved to suppress all of the evidence seized as a result of the NIT warrant (dkt. no. 43), arguing it violated Fed. R. Crim. P. 41(b) because it was for a search outside the magistrate judge's jurisdictional limit and, consequently was void ab initio. As such, he contends no good faith or other exceptions would apply and suppression of any evidence gathered as a result of its execution is therefore appropriate.

The government contends that the warrant was authorized under Fed. R. Crim. P. 41(b)(4) because the NIT was a form of tracking device. Alternatively, even if the NIT warrant violated Rule 41, it argues that this was a mere technical violation that does not rise to the level of a constitutional violation necessary to justify suppression. Finally, the government argues that, even if the

warrant is void ab initio, the exigent circumstances exception would render a warrantless search reasonable in this case.

II. APPLICABLE LAW

A. Fourth Amendment

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Searches subject to Fourth Amendment protections are those in which the "government violates a subjective expectation of privacy that society recognizes as [objectively] reasonable." United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc) (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

B. Federal Rule of Criminal Procedure 41(b)

Fed. R. Crim. P. 41 (b) provides in pertinent part:

> At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;

. . .

> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; . . . .

III. DISCUSSION

The NIT warrant in this case has been the subject of numerous motions to suppress filed by defendants in federal courts throughout the United States.[3] For varying reasons, the vast majority of courts addressing the issue have found suppression unwarranted. The initial question presented here is whether Lough had the kind of reasonable expectation of privacy in his IP address that society is prepared to recognize. Assuming he did have such an expectation, the question becomes whether the NIT warrant constituted a search outside of the

[3]See, e.g., United States v. Scarborough, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016); United States v. Jean, 2016 WL 4771096 (W.D. Ark, Sept. 13, 2016); United States v. Henderson, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); United States v. Croghan, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); United States v. Ammons, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); United States v. Torres, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); United States v. Acevedo-Lemus, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); United States v. Eure, 2016 WL 4059663 (E.D. Va. July 28, 2016); United States v. Matish, 2016 WL 3545776 (E.D. Va. June 23, 2016); United States v. Darby, 2016 WL 3189703 (E.D. Va. June 3, 2016); United States v. Weredene, 2016 WL 3002376 (E.D. Pa. May 18, 2016); United States v. Levin, 2016 WL 2596010 (D. Mass. May 5, 2016); United States v. Michaud, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

Eastern District of Virginia that went beyond the magistrate judge's territorial authority under Rule 41(b). Finally, the Court must examine whether any exigent circumstances or the Leon good faith exception counsel against suppression.

A. Reasonable Expectation of Privacy

Lough had no reasonable expectation of privacy in his IP address. To establish that he had a legitimate expectation of privacy, Lough must first demonstrate that he had a "subjective expectation of privacy." United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). That subjective expectation of privacy must be one that is "objectively reasonable; in other words, it must be an expectation that society is willing to recognize as reasonable." U.S. v. Castellanos, 716 F.3d 828, 832 (4th Cir. 2013) (quoting United States v. Bullard, 645 F.3d 237, 242 (4th Cir. 2011) (internal quotation marks omitted)). Absent a legitimate expectation of privacy, Lough cannot invoke the protections of the Fourth Amendment.

The third party doctrine holds that "an individual can claim no legitimate expectation of privacy in information that he has voluntarily turned over to a third party," because when he "reveal[s] his affairs to another, [he] takes the risk . . . that the information will be conveyed by that person to the Government."

Graham, 824 F.3d at 427 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979) and United States v. Miller, 425 U.S. 435, 443 (1976)). The doctrine applies with equal force even in those instances in which the individual reveals such information "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Id. quoting Miller, 425 U.S. at 443.

Lough could not have had a subjective expectation of privacy because he voluntarily turned over his IP address to every computer with which he made contact, including the first node of the TOR network. Although he may have wished to remain anonymous, and even hoped that the TOR would facilitate that goal, hoping and wishing are not the equivalent of expecting a certain result. At the very least, Lough certainly knew that he was revealing his IP address to one unknown third party who, for all he knew, was a law enforcement officer.[4] Indeed, Lough's IP address was used by a third party before the NIT ever reached his computer, because the final node in

[4]Tellingly, the TOR project, which supplies the software and platform that Lough utilized to visit the Playpen website, warns users that sites they visit through TOR could see their identifying information: "Tor cannot solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want sites you visit to see your identifying information." See https://www.torproject.org/about/overview.html.en#stayinganonymous, last visited November 7, 2016.

the anonymizing circuit necessarily had to know his IP address to make the final connection on the data's return trip.

Even assuming that Lough did have a subjective expectation of privacy, it is not one that society is prepared to recognize as reasonable. Castellanos, 716 F.3d at 832. Courts have repeatedly held that there is no objectively reasonable expectation of privacy in one's IP address:

> Even if [the defendant] could show that he had a subjective expectation of privacy in his subscriber information, such an expectation would not be objectively reasonable. Indeed, "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."

U.S. v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases)).[5] Accordingly, in accord with the numerous other district

[5]See also United States v. Wheelock, 772 F.3d 825, 828-29 (8th Cir. 2014)(finding that the government's acquisition of the defendant's IP address through a third-party subpoena to his internet service provider did not violate the Fourth Amendment); United States v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013) (finding no privacy interest in defendant's IP address); U.S. v. Christie, 624 F.3d 558, 573–74 (3rd Cir. 2010) (concluding that "no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [internet service providers]").

courts that have addressed this issue, this Court concludes that Lough had no legitimate expectation of privacy in his IP address.[6]

Clearly, Lough does have a privacy interest in his home and its contents, including his computer. Nevertheless, the FBI's use of the NIT to discover Lough's IP address was not a search of the contents of that computer. The Supreme Court of the United States has "forged a clear distinction between the contents of communications and the non-content information that enables communications providers to transmit the content." United States v. Graham, 824 F.3d at 433.

In Graham, the Fourth Circuit applied this distinction to cell-site location information ("CSLI") and concurred with the Sixth Circuit that "CSLI is non-content information because 'cell-site data – like mailing addresses, phone numbers, and IP addresses – are information that facilitate personal communications, rather than part of the content of those communications themselves.'" Graham,

[6]See, e.g., Werdene, 2016 WL 3002376 at *9 ("[The defendant] was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information."); Michaud, 2016 WL 337263 at *7 ("Even though it was difficult for the Government to secure that information tying the IP address to [defendant], the IP address was public information, like an unlisted telephone number, and eventually could have been discovered."); Jean, 2016 WL 4771096 at *7-10 (holding that a search warrant to retrieve the defendant's IP address was unnecessary); Matish, 2016 WL 354776 at *22-24 (same); Acevedo-Lemus, 2016 WL 4208436 (same).

824 F.3d at 433 (emphasis added) (quoting United States v. Carpenter, 819 F.3d 880, 887–88 (6th Cir. 2016)). The Graham court noted that, for each case dealing with communications using a particular medium and subsequently protecting the content of those communications, there was a concomitant ruling "expressly withholding Fourth Amendment protection from non-content information." Id. (emphasis in original). Consequently, just as "[i]t blinks at reality [] to hold that CSLI, which contains no content, somehow constitutes a communication of content for Fourth Amendment purposes," it is unassailable that the NIT did not conduct a search of the contents of Lough's computer. Id. at 434.

In sum, Lough had no expectation of privacy in his IP address because he knowingly exposed it to third parties. Furthermore, the NIT did not conduct a search of the content of his computer such that it was subject to Fourth Amendment protections. The Court therefore denies Lough's motion to suppress.

B. Validity of the Warrant

Lough asserts that Rule 41(b)(1) did not authorize the magistrate judge in the Eastern District of Virginia to issue a warrant to search his computer in West Virginia. Further, he contends that no other subsections of Rule 41(b) provided such

authorization and the warrant was therefore void ab initio.[7] Finally, Lough maintains that the violation of Rule 41(b) was of such constitutional dimension as to require suppression. The government counters that argument by asserting that the NIT is akin to a tracking device, and, as such, is authorized under Rule 41(b)(4). Rule 41(b)(4) provides that "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both."

The Court agrees with Lough that the clear language of subsection (1) explicitly limits the magistrate's "authority to issue a warrant to search for and seize a person or property" to only those persons or property "located within the district." Fed. R. Crim. P. 41(b)(1). Here, as neither Lough nor his computer was

[7]Lough also argues that the warrant violated the Federal Magistrates Act, 28 U.S.C. § 636(a), which provides similar jurisdictional limitations on the warrant power of magistrate judges. Under 28 U.S.C. § 636(a)(1), however, the Act expands magistrate's jurisdiction to include "elsewhere as authorized by law--(1) all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." Thus, because § 636(a)(1) clearly allows the Rules of Criminal Procedure to expand the jurisdictional sphere of a magistrate judge's authority, the Court's inquiry here is limited to what Fed. R. Crim. P. 41(b) authorized in this case.

located in the Eastern District of Virginia, Rule 41(b)(1) did not authorize the NIT warrant.

Nevertheless, because the NIT is analogous to a tracking device in both function and effect, the magistrate judge was authorized under Rule 41(b)(4) to issue a warrant for its use. Rule 41(b)(2) specifically incorporates 18 U.S.C. § 3117(b), which defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Despite any further statutory definition of a "device," "it is a word commonly used to describe 'a tool or technique used to do a task.'" Jean, 2016 WL 4771096, at *16 (citing Device, American Heritage Dictionary, http://www.yourdictionary.com/device#americanheritage (last visited September 12, 2016)).

The district court in United States v. Jean, tallied the courts that have specifically addressed whether the NIT was akin to a tracking device such that Rule 41(b)(4) would authorize a warrant for its implementation. 2016 WL 4771096, at *14-16. Although not all courts agree, the reasoning of those courts that have likened users of the Playpen site to individuals making a "virtual trip" into the district is compelling.[8] The court in Jean found, for example, that

[8]See Jean, 2016 WL 4771096, at *15-16 (finding that the defendant had made a virtual trip to the Eastern District of Virginia); Darby, 2016 WL 3189703 at *12 (E.D.Va. June 3, 2016) (opining that "[u]sers of Playpen digitally touched down in the

the NIT qualified as an "electronic device" as defined in 18 U.S.C. § 3117(b) "because it is an investigative tool consisting of computer code transmitted electronically over the internet." Id. It further found that, in accord with Rule 41(b)(4), the NIT's purpose was to track the movement of "'property'—which in this case consisted of intangible 'information,' something expressly contemplated by the definition in Rule 41(a)(2)(A)."[9]

The court then addressed the final requirement, that the device be "install[ed]" within the district. First, it recognized the "problematic" nature of the requirement, given that the NIT was an intangible device, tracking intangible information, a factor that raised questions regarding the locus of the installation. Id. at *16. From the evidence before it, the court concluded that the installation of the NIT did not occur at the user's remotely located

---

Eastern District of Virginia when they logged into the site" and the NIT warrant authorized something "exactly analogous" to the installation of a traditional tracking device); Eure, 2016 WL 4059663 (same); Matish, 2016 WL 3545776 at *18 ("[W]henever someone entered Playpen, he or she made 'a virtual trip' via the Internet to Virginia." . . . When the computer left Virginia—when the user logged out of Playpen—the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target's location.")

[9]Rule 41(a)(2)(A) defines "Property" to "include[] documents, books, papers, any other tangible objects, and information." (emphasis added).

computer, but rather at the server located in the Eastern District of Virginia. Id. at *16-17.

The Court agrees with this analysis. The NIT was imbedded in the material Lough sought to download; he came to the server to get the material; the server did not reach out to him unsolicited. See Id. at 17 ("It is also undisputed that *but for* Mr. Jean electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed." (emphasis in original)). Based on this, it is clear that the installation of the NIT occurred at the server in the Eastern District of Virginia.

A summary of the physical and virtual facts concerning how the NIT was employed is helpful. Lough took a virtual trip to the Eastern District of Virginia, but rather than travel by car, he traveled digitally – his vehicle was comprised of packets of information. Once there, the FBI attached a digital electronic tracking device to those packets, which Lough virtually rode back to the Northern District of West Virginia. Upon his virtual return, Lough parked his digital vehicle built of those packets of information on his computer, rather than in his driveway. At that point, the NIT sent back his digital address, just as a GPS tracker would send back his coordinates. Accordingly, the NIT is analogous to a tracking device authorized under Rule 41(b)(4), and the NIT

warrant is an information-tracking warrant that comports with Rule 41(b)(4), which Magistrate Judge Buchanan had the authority to issue.

C. The Alleged Violation of Rule 41(b) was Technical

Even if the NIT warrant violated Rule 41(b), suppression is not warranted here. In United States v. Simmons, the Fourth Circuit opined that "[t]here are two categories of Rule 41 violations: those involving constitutional violations, and all others." 206 F.3d 392, 403 (4th Cir. 2000) (citations omitted). Violations that are non-constitutional in nature "warrant suppression only when the defendant is prejudiced by the violation," or when "there is evidence of intentional and deliberate disregard of a provision in the Rule." Id. (internal quotations and citations omitted).

By definition, a constitutional violation occurs when a warrant offends the protections afforded under the Fourth Amendment, which mandates that the judge issuing the warrant do so based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., amend. IV.

There was no constitutional violation here. The parties do not argue, nor has any court found, that the NIT warrant lacked probable cause. The FBI affidavit provided to Magistrate Judge Buchanan included a lengthy, detailed description of the content and

operational nature of the Playpen website, as well as of the process by which users accessed the site and its materials. Lough, however, argues that the NIT warrant did not meet the particularity requirement. Citing United States v. Bonner, he contends that, contrary to the "manifest purpose of the particularity requirement . . . to prevent wide-ranging general searches by police," the NIT warrant was too vague to "prevent a reasonable probability that another premise might be mistakenly searched." 808 F.2d 864, 866 (1st Cir. 1986).

The FBI affidavit belies this contention. It clearly explained that only those users who affirmatively sign into the Playpen site using their screen name and password would have the NIT attached to their requested downloads of information from the site. The NIT warrant searched the server in the Eastern District of Virginia for users who were specifically visiting the site and, even more specifically, only for those users who explicitly requested that information be sent to their computers by way of downloaded pictures and videos. This is a far cry from a "wide ranging general search" that might mistakenly search some unaffiliated computer. Id. Accordingly, the NIT warrant possessed the requisite particularity to satisfy the Fourth Amendment.

Notwithstanding the absence of a constitutional violation, the Court must still determine whether any non-constitutional violation

of Rule 41(b) occurred that would warrant suppression. Suppression is warranted only if Lough was "prejudiced by the violation," or when "there is evidence of intentional and deliberate disregard of a provision in the Rule." Simmons, 206 F.3d at 403.

Lough contends that he was prejudiced because the "search authorized by the Residential Warrant would not have occurred but for the information derived from the improperly issue NIT warrant." Dkt. No. 43 at 13. What he overlooks, however, is that, even had the magistrate judge concluded she lacked authority under Rule 41(b) to issue the warrant, the FBI could have simply presented it to the district court judge in that same district. See Jean, 2016 WL 4771096 at *18 (noting that "both parties appear to agree . . . that an Article III judge in the Eastern District of Virginia could have authorized this particular search warrant"). Indeed, even the holding of Levin, upon which Lough relies so heavily and which provided the impetus for his motion to suppress, recognized that "[s]ection 636(a) [of the Federal Magistrates Act] and Rule 41(b) limit the territorial scope of magistrate judges - they say nothing about the authority of district judges to issue warrants to search property located outside their judicial district." 2016 WL 2596010 at *14 (emphasis in original). Consequently, Lough was not prejudiced; even had the magistrate exceeded her jurisdictional

authority, the agents could have employed an alternative legal means of securing the warrant.

Nor was there any "evidence of intentional and deliberate disregard of a provision in the Rule." Simmons, 206 F.3d at 403. On the contrary, the FBI Special Agent prepared a lengthy affidavit replete with highly detailed and specific information to present to Magistrate Judge Buchanan. There is no legitimate dispute that any of the information contained in the affidavit was false or materially misleading, or that it lacked the requisite probable cause.

There is also no evidence that Magistrate Judge Buchanan abdicated her judicial duty by simply acting as a "rubber stamp for the [FBI]." Leon, 468 U.S. at 914. Moreover, any argument that she knew she lacked authority to issue the NIT warrant under Rule 41(b), and therefore intentionally or deliberately disregarded the Rule, lacks merit. Indeed, the mere fact that so many district court judges around the nation are now struggling with this same issue demonstrates its complexity and uncertainty.

In summary, the Court concludes that any violation of Rule 41(b) alleged by Lough was not constitutional in nature; any jurisdictional defect in the magistrate judge issuing the warrant was not prejudicial to Lough because a district judge could have issued the same warrant; and, finally, the magistrate judge did not

intentionally and deliberately disregard a provision in the Rule. Consequently, suppression is not required in this case.

D. Exceptions to the Exclusionary Rule

Assuming, arguendo, that a Fourth Amendment violation occurred in the issuance or execution of the NIT warrant, the Court nonetheless must analyze "whether suppression is the proper remedy." See U.S. v. Davis, 690 F.3d 226, 251 (4th Cir. 2012) (citing Leon, 468 U.S. at 906 ("Whether the exclusionary sanction is appropriately imposed in a particular case ... is an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct.").

The exclusionary rule is a drastic remedy that exacts a high social cost. See Nix v. Williams, 467 U.S. 431, 442 (1984); Rakas v. Illinois, 439 U.S. 128, 137 (1978) (recognizing that "[e]ach time the exclusionary rule is applied it exacts a substantial social cost for the vindication of Fourth Amendment rights."). "The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free — something that 'offends basic concepts of the criminal justice system.'" Herring v. U.S., 555 U.S. 135, 141 (2009) (quoting Leon, 468 U.S. at 908). Consequently, defendants seeking to invoke the exclusionary rule face a "high obstacle" due to "the rule's costly toll upon truth-seeking and law

enforcement objectives." Id. (quoting Pennsylvania Bd. of Probation and Parole v. Scott, 524 U.S. 357, 364-65 (1998)). The paramount purpose of the exclusionary rule is deterrence; ultimately, courts should only apply the exclusionary rule when "the benefits of deterrence [] outweigh the costs." Id. (citing Leon, 468 U.S. at 910).

To help counteract the drastic nature of the exclusionary rule, the Supreme Court in Leon articulated the "good faith" exception. Davis, 690 F.3d at 251. The good faith exception counsels that "[w]hen police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant." Herring, 555 U.S. at 142 (quoting Leon,468 U.S. at 922). Since Leon, the Supreme Court has broadened the reach of the good faith exception beyond those cases where warrants, in retrospect, lacked probable cause. See U.S. v. Davis, 690 F.3d 226, 251 (4th Cir. 2012)("The Supreme Court's recent decisions applying the exception have broadened its application . . . .").[10]

[10]See also, e.g., Davis v. U.S., 564 U.S. 229 (2011) (applying good faith exception when police conducted a search in compliance with binding precedent that is later overruled); Herring v. U.S., 555 U.S. 135 (2009) (applying good faith exception to arrest of defendant based on warrant that had been rescinded five months earlier); Arizona v. Evans, 514 U.S. 1, 14 (1995) (applying good

Normally, a warrant issued by a neutral magistrate judge is sufficient to establish that the law enforcement officer has "acted in good faith in executing the search," so long as his "reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant [is] objectively reasonable." Leon, 468 U.S. at 921-22 ("[O]nce the warrant issues, there is literally nothing more the policeman can do in seeking to comply with the law.").

The Supreme Court has been abundantly clear that "the reach of the exclusionary rule does not extend beyond police conduct to punish the mistakes of others, be they judicial officers or employees, or even legislators." U.S. v. McCane, 573 F.3d 1037, 1045 (10th Cir. 2009).[11]

---

faith exception to arrest by police who reasonably relied on erroneous information entered by a court employee into a court database that an arrest warrant was outstanding); Illinois v. Krull, 480 U.S. 340 (1987) (applying good faith exception to warrantless administrative searches performed in good-faith reliance on a statute later declared unconstitutional).

[11] In support, McCane cites Arizona v. Evans, 514 U.S. 1, 14 (1995) ("[T]he exclusionary rule was historically designed as a means of deterring police misconduct, not mistakes by court employees."); Illinois v. Krull, 480 U.S. 340, 350 (1987) ("We noted in Leon as an initial matter that the exclusionary rule was aimed at deterring police misconduct. Thus, legislators, like judicial officers, are not the focus of the rule." (citation omitted)); and Leon, 468 U.S. at 916 ("[T]he exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates.").

Importantly, the Supreme Court has explained why the exclusionary rule does not apply to mistakes by judicial officers:

> First, the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates. Second, there exists no evidence suggesting that judges and magistrates are inclined to ignore or subvert the Fourth Amendment or that lawlessness among these actors requires application of the extreme sanction of exclusion.
>
> Third, and most important, we discern no basis, and are offered none, for believing that exclusion of evidence seized pursuant to a warrant will have a significant deterrent effect on the issuing judge or magistrate. Many of the factors that indicate that the exclusionary rule cannot provide an effective "special" or "general" deterrent for individual offending law enforcement officers apply as well to judges or magistrates. And, to the extent that the rule is thought to operate as a "systemic" deterrent on a wider audience, it clearly can have no such effect on individuals empowered to issue search warrants. Judges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers, they have no stake in the outcome of particular criminal prosecutions. The threat of exclusion thus cannot be expected significantly to deter them. Imposition of the exclusionary sanction is not necessary meaningfully to inform judicial officers of their errors, and we cannot conclude that admitting evidence obtained pursuant to a warrant while at the same time declaring that the warrant was somehow defective will in any way reduce judicial officers' professional incentives to comply with the Fourth Amendment, encourage them to repeat their mistakes, or lead to the granting of all colorable warrant requests.

Leon, 468 U.S. at 916; See also Davis v. U.S., 564 U.S. at 239 (noting that "'punish[ing] the errors of judges' is not the office of the exclusionary rule" (quoting Leon)).

The good faith exception is not without limits, however. Courts have identified the following four circumstances where it should not apply:

> (1) [T]he magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
> (2) [T]he issuing magistrate wholly abandoned his judicial role . . . ;
> (3) [T]he affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and
> (4) [U]nder the circumstances of the case the warrant is so facially deficient, i.e., in failing to particularize the place to be searched or the things to be seized that the executing officers cannot reasonably presume it to be valid.

U.S. v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotations and citations omitted).

Critically, in the Fourth Circuit, the "flagrancy of police misconduct" is a determinative factor in analyzing the propriety of applying the exclusionary rule. Davis, 690 F.3d at 251. Indeed, absent police culpability, the good faith exception will invariably operate to defeat exclusion. See id. ("[I]n 27 years of practice under Leon's good-faith exception, we have 'never applied' the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct.'" (quoting Davis, 564 U.S. at 240)).

Lough argues that because Magistrate Judge Buchanan lacked authority to issue the NIT warrant beyond her jurisdiction it is void ab initio, making the good faith exception inapplicable. In support, he cites Levin, which differentiated between a warrant that was subsequently invalidated and a warrant that was "void at its outset," finding the latter to be "no warrant at all." 2016 WL 2596010, *4 (citing U.S. v. Krueger, 809 F.3d 1109, 1118 (10th Cir. 2015)).

In Levin, the district court began by noting that the applicability of the good faith exception to a warrant that was void ab initio was a matter of first impression in the First Circuit, and that no Supreme Court decisions post-Leon had specifically dealt with the issue. Id. at *11. It went on to recognize that the Sixth Circuit was the only Circuit Court to address whether the good faith exception applied to a warrant void ab initio.

As part of that discussion, Levin analyzed United States v. Scott, 260 F.3d 512 (6th Cir. 2001), the first of the Sixth Circuit cases to discuss warrants issued without authority and thus void ab initio. In Scott, the circuit court held that exclusion was proper where the warrant had been issued by a retired judge who lacked the authority to do so. Nine years later, in United States v. Master, 614 F.3d 236, 241 (6th Cir. 2010), the Sixth Circuit reversed its decision in Scott, holding that, even though the warrant was void

for lack of authority, as was the case in Scott, the good faith exception precluded suppression because Scott's reasoning was "no longer clearly consistent with Supreme Court doctrine." Master, 614 F.3d at 242. Expanding on its new thinking, the Sixth Circuit recognized that "[t]he Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, 'the benefits of deterrence must outweigh the costs.'" Id. at 243 (quoting Herring, 555 U.S. 135, 142 (2009)).

In Levin, although the district court was not bound by the rulings in either Scott or Master, it chose to follow the reasoning in Scott. Id. at *12. In light of the holding of the Supreme Court in Herring, however, the reasoning of the Sixth Circuit in Master is more persuasive. Therefore, whether the warrant is void ab initio or voided at a later date is immaterial to the question presented. The true measure of whether the good faith exception applies under Leon is determined by balancing the deterrent effect against the societal costs. See Herring, 555 U.S. at 141.[12]

A review of the facts of this case establishes that no circumstances exist that warrant exclusion. The FBI agents acted

[12]This view also makes more sense when looking at the Supreme Court decisions. For example, justifying exclusion when a warrant is void ab initio, but inclusion when a warrant is non-existent, as in Herring, would require some semantic gymnastics.

responsibly, providing the magistrate judge with a highly detailed affidavit that clearly established probable cause. Furthermore, there is no evidence that the magistrate judge abandoned her judicial role, or that the warrant was so facially invalid that the executing agents could not presume it to be valid. Nor is there any evidence that the FBI agent swore to anything in the affidavit that he knew to be false or would have known to be false except for his reckless disregard of the truth. At bottom, there simply is no misconduct here, a fact that ultimately dooms Lough's motion. See Davis, 564 U.S. at 240 ("Under our exclusionary-rule precedents, this acknowledged absence of police culpability dooms Davis's claim."). There is little deterrent effect available by suppressing the evidence, yet the societal costs of doing so would be significant. For these reasons, therefore, the Court finds that the good faith exception applies and denies Lough's motion to suppress.[13]

V. CONCLUSION

For the reasons discussed, the Court concludes as follows:

1) Lough had no reasonable expectation of privacy in his IP address, nor did the NIT constitute a Fourth

[13]The government posits that the exigent circumstances exception applies to bar suppression. After review, the Court finds this theory unpersuasive, but nonetheless denies suppression for the other reasons stated.

Amendment search of the content of his computer; thus, a warrant was unnecessary;

2) Even so, the NIT warrant complied with Rule 41(b)(4) because the NIT is sufficiently akin to a tracking device;

3) Moreover, any violation of Rule 41(b) was non-constitutional in nature, and there was no prejudice to Lough, nor any evidence of intentional and deliberate disregard of the Rule; and

4) Finally, the good faith exception renders suppression improper in this case.

Accordingly, the Court **DENIES** Lough's motion to suppress.

It is so **ORDERED**.

The Court directs the Clerk to transmit copies of this order to counsel of record and all appropriate agencies.

DATED: November 18, 2016

/s/ Irene M. Keeley
IRENE M. KEELEY
UNITED STATES DISTRICT JUDGE